



Secure from the START

Phoenix TrustConnector™ 2

Seamless Device Identity and Strong Authentication for Windows® Environments

Strong Device Identification

Tamper-resistant Digital Credentials

Identity Theft Prevention

In today's networked computing environments, user authentication is simply not enough. Thieves using stolen credentials can access your network from practically any device. And, employees with valid IDs and corrupted devices can wreak havoc on your network. Every time a connection is made to your network, you need to identify both your users and your devices.

Phoenix TrustConnector 2 provides a cost-effective, easy-to-implement, software-only solution for knowing both through device authentication. TrustConnector 2 creates a unique device key that cannot be altered or stolen. And it safeguards your business against credential sharing and digital identity theft.

TrustConnector 2 incorporates valuable security features previously found only in proprietary, hardware-based strong authentication solutions:

- **Key Storage:** Uses native x86 system hardware attributes on legacy systems to strongly encrypt and strengthen storage for private keys.
- **Device Authentication:** Multi-factor user/device authentication is now a reality for all Windows environments through our built-in prevention of private-key copying, and by ensuring that the key is associated with only its host device.
- **Seamless Microsoft Integration:** Fully integrated with Microsoft CryptoAPI to support any digital certificate-aware Microsoft and Microsoft-certified partner application.
- **Easy Deployment:** Easy to deploy, highly scalable, and does not require additional hardware unlike traditional "hardware based authentication" solutions like tokens and smart cards.



The Phoenix Advantage: Innovation at the System Core

Phoenix Technologies, as a worldwide innovator in core systems software (CSS), provides a unique vision to help transparently identify users as they connect to the network. TrustConnector 2 implements this vision by tightly binding user and computer certificates to the device, thus providing strong device identification and enhancing the protection of digital credentials on the devices.

TrustConnector intelligently uses characteristics of the hardware on any x86 architecture PC to “harden” digital credentials. Thus, TrustConnector 2 provides platform-secured methods for protecting the device identity and ensures that credentials belong to and can be used only on the system to which they are issued. And if the system comes with Phoenix TrustedCore or Phoenix FirstBIOS CSS, it will provide even greater assurance by taking advantage of the CSS-embedded crypto engine and secure silicon to lock down private keys below the OS. Alternatively, if the system is equipped with a TPM device, TrustConnector 2 can use the TPM resources for cryptography and secure storage.

Improve the effectiveness of existing security infrastructure by incorporating device profile and validation/authentication for VPN, wireless access, SSL-based network connections and certificate-aware applications.

Reduce the risk of data and intellectual property theft by protecting the keys for certificate-based applications and binding them to device-specific profiles. Even in the unlikely event that the keys were stolen, they could not work on another device.

Lever age your existing security investment because TrustConnector 2 is non-disruptive, so it requires minimal changes to your network infrastructure to enable device authentication on the network.

Enable device access policy enforcement to reduce the risk of threats and vulnerabilities from unknown devices accessing the enterprise networks and threatening to compromise data and interrupt business operations.

Benefits:

- Allows enforcement of a device-specific security policy
- Provides strong, tamper-resistant storage of digital credentials
- Helps prevent data theft, business interruption, hacking, and other threats
- Offers seamless compatibility with existing security products
- Easy to deploy and manage so it's a cost effective solution
- Can be installed on new or existing machines
- Submitted for FIPS 140-1 Level 1 Certification
- Supports TPM-enabled CSPs from IBM, Wave Systems and Infineon
- Delivers the promise of trusted computing today!

Client Requirements:

- Windows XP Pro/Home (No SP, SP1 or SP2)
- Windows 2000 (No SP*, SP1*, SP2, SP3 or SP4)
- Pentium II or later

*Requires High Encryption Pack

For the latest technical specifications visit us at www.phoenix.com

Secure from the START

Phoenix Technologies is a global market leader in device-defining software that enables endpoint security from the start. The company first established dominant industry leadership over 25 years ago with BIOS software. From this unique foundation of core level expertise and firmware offering the highest levels of reliability, Phoenix has created a portfolio of innovative software products that simply and easily identify and restore devices, thereby assuring users unparalleled endpoint security and availability.

Phoenix Technologies Ltd.

915 Murphy Ranch Road
Milpitas, CA 95035 USA
408.570.1000 main
408.570.1001 fax

800.446.9202 North America sales
781-BUY PTEC Outside North America sales

©2006 Phoenix Technologies Ltd. Phoenix and Phoenix Technologies are registered trademarks of Phoenix Technologies Ltd. All rights reserved worldwide. All other brand or product names are the trademarks and property of their respective holders.

